AO 106 (Rev. 04/010) Application for Search Warrant AUTHORIZED AND APPROVED/DATE: s/Brandon Hale 11/16/2022

UNITED STATES DISTRICT COURT

for the

WESTERN DISTRICT OF OKLAHOMA

AMG 11/17/22

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
Black Samsung Cell Phone with IMEI: 353967950684376

Case No: M-22-832-AMG

APPLICATION FOR SEARCH WARRANT

I, a federal law enforcement officer or attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following property *(identify the person or describe property to be searched and give its location)*:

See Attachment A, which is attached and incorporated by reference.

Located in the Western District of Oklahoma, there is now concealed (*identify the person or describe the property to be seized)*:

See Attachment A, which is attached and incorporated by reference.

The basis for the search under Fed. R. Crim.P.41(c) is (*check one or more*):

- ☒ evidence of the crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §2252A	Possession and distribution of child pornography

The application is based on these facts:

See attached Affidavit of Special Agent Marisol Flores, Federal Bureau of Investigation, which is incorporated by reference herein.

- ☒ Continued on the attached sheet(s).
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet(s).

Applicant's signature

Marisol Flores
Special Agent
Federal Bureau of Investigation

Sworn to before me and signed in my presence.

Date: 11/17/22

Judge's signature

City and State: Oklahoma City, OK

Amanda Maxfield-Green, U.S. Magistrate Judge
Printed name and title

THE UNITED STATES DISTRICT COURT FOR THE WESTERN DISTRICT OF OKLAHOMA

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Marisol Flores, a Special Agent with the Federal Bureau of Investigation (FBI), Oklahoma City, Oklahoma, being duly sworn, depose and state as follows:

1. I have been employed as a Special Agent of the FBI since May 2015, and have been assigned to the Oklahoma City FBI Field Office. During that time, I have conducted a wide variety of investigations, including numerous cases involving child pornography and sexual exploitation of children.

2. As a Special Agent, I am authorized to investigate violations of the laws of the United States and to execute warrants issued under the authority of the United States.

3. The information contained in this affidavit is based upon my personal knowledge and observation, my training and experience, conversations with other law enforcement officers and witnesses, and review of documents and records. This affidavit is made in support of an application for a warrant to search the cell phone seized from Jason Roberts's person (hereinafter referred to as "the SUBJECT DEVICE"), which is described in detail in Attachment A to this affidavit for the items specified in Attachment B hereto, which constitute instrumentalities, fruits, and evidence of violations of 18 U.S.C. § 2252A.

4. This investigation, described more fully below, has revealed that an individual knowingly utilized the BitTorrent peer-to-peer (P2P) file-sharing network from 8104 W Britton Rd., Oklahoma City, Oklahoma, the SUBJECT PREMISES, to possess and distribute child pornography in violation of 18 U.S.C. §§ 2252A(a)(5)(B) and 2252A(a)(2), and that there is probable cause to believe that evidence, fruits, and instrumentalities of such violations are located

on the SUBJECT DEVICE.

5. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me regarding this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to support the issuance of a search warrant.

TERMS

6. Based on my training and experience, I use the following technical terms and definitions:

a. An Internet Protocol (IP) address is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range of 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static, or long-term, IP addresses. Other computers have dynamic, or frequently changing, IP addresses.

b. Single-source download applies to a file that is downloaded from one IP address only. In P2P software, users often download different parts of the same file from many other users at once in an attempt to gain the file quicker. A single-source download comes from one user/IP address instead.

BACKGROUND ON P2P FILE SHARING

7. A growing phenomenon on the Internet is P2P file sharing. P2P file-sharing software is designed to allow users to trade digital files through a worldwide network that is formed by linking computers together.

8. To access the P2P networks, a user first obtains the P2P software from the Internet. This software is used exclusively for the purpose of sharing digital files. In general, P2P software allows the user to set up file(s) on his/her computer so that the files can be shared with others running compatible P2P software. In essence, a user allows his/her computer to be searched and accessed by other users of the network. If another user finds a file of interest on his/her computer, the other user may download that file. A user obtains files by opening the P2P software on his/her computer and conducting keyword searches of the P2P network. The P2P software then conducts a search of all computers connected to that network to determine whether any files matching the search term(s) are currently being shared by any other user on that network.

9. BitTorrent, one type of P2P software, sets up its searches by keywords, typically on torrent websites. The results of a keyword search are displayed to the user. The website does not contain the actual files being shared, only the file referred to as a ".torrent" file. The user then selects one or more .torrent files from the results for download. The .torrent files contain instructions on how a user can download the file(s) referenced in the torrent. The download of file(s) referenced by the .torrent file is achieved using a BitTorrent client/program, through a direct connection between the computer requesting the file(s) and the computer(s) sharing the actual file(s) (not the .torrent file but the actual files referenced in the .torrent file, using any BitTorrent client/program).

10. For example, a person interested in obtaining images of child pornography would open the BitTorrent website or program on his/her computer and conduct a keyword search for files using a term such as "preteen sex." The results of the search are returned to the user's computer and displayed on the torrent site. The user then selects a .torrent from the results displayed. The .torrent file is the set of instructions a BitTorrent client/program needs to find the files referenced

in the .torrent file. Once the .torrent file is downloaded, it is used by a BitTorrent client/program, previously downloaded and installed by the user, to download the actual files. The actual file(s) are downloaded directly from the computer or computers sharing the file(s). The download is achieved via the Internet. The downloaded file(s) are then downloaded/stored in an area previously designated by the user and/or the software. The downloaded files will remain until moved or deleted.

11. A P2P file transfer is assisted by reference to an IP address, which provides a unique location making it possible for data to be transferred between computers. The computer running the file sharing application, in this case a BitTorrent application, has an IP address assigned to it while it is on the Internet. BitTorrent users are able to see the IP address of any computer system sharing files to them or receiving files from them.

12. Law enforcement officers using BitTorrent log the IP address which has sent the files or information regarding files being shared. Investigators can then search public records, such as ARIN, that are available on the Internet to determine the Internet service provider who has assigned that particular IP address. Based upon the IP address, investigators can obtain subscriber information from the Internet service provider. The subscriber information identifies the individual to whom the Internet service account is registered.

13. One of the advantages of P2P file sharing is that multiple files may be downloaded in parallel. This means that the user can download more than one file at a time. In addition, a user may download parts of one file from more than one source computer at a time. For example, a BitTorrent user downloading an image file may actually receive parts of the image from multiple computers/sources. The advantage of this is that it speeds up the time it takes to download the file. However, software used by the FBI to download files from P2P networks will only download from

a single source, via a direct connection (i.e., a single source download).

14. The computers that are linked together to form the P2P network are located throughout the world; therefore, the P2P network operates in interstate and foreign commerce. A person who shares child pornography files on a P2P network is hosting child pornography and therefore is promoting, presenting, and potentially distributing child pornography.

15. Even though the P2P network links together computers from all over the world and users can download files, it is not possible for one user to send or upload a file to another user of the P2P network. The software is specifically designed to only allow the download of files that have been selected. A user does not have the ability to send files from his/her computer to another user's computer without their permission or knowledge. Therefore, it is not possible for one user to send or upload child pornography files to another user's computer without his/her active participation.

BACKGROUND OF INVESTIGATION

16. This case originated on July 13, 2022, when law enforcement conducted an online undercover investigation to identify individuals possessing and sharing child pornography on the Internet using the BitTorrent P2P network. Law enforcement used a P2P file-sharing program that utilizes a single-source download process. Based upon training and experience, I was familiar with P2P file-sharing, specifically the operation of the BitTorrent network. Law enforcement directed their focus to a computer using IP address 68.12.239.130 because it was associated with a torrent file which referenced 31 files, at least one of which had been identified as a file of interest in child pornography investigations.

17. On July 13, 2022, between 17:56 and July 14, 2022 at 01:40 hours, Central Standard Time, law enforcement completed single-source downloads of approximately 26 files that the

device using IP address 68.12.239.130 was making available for others to download on the BitTorrent network. Each of the files was downloaded directly from the device using IP address 68.12.239.130. Based upon my training and experience, I determined several of these files depict children under the age of eighteen years engaged in lascivious exhibitions of the genitals that constitute child pornography as defined by Title 18, U.S.C. § 2256. Two of these files are described below:

a. Filename: 2014 2013 9Yo Latin Bitch Does All Mvx 1855 Pthc Center) (Opva).wmr
Description: This video depicts a prepubescent female, wearing only a blue shirt and nothing else. She is performing oral sex on the erect penis of what appears to be an adult male. Next in the video, the adult male lifts up the girl and places her on top of his naked body where his erect penis is rubbing her vagina and anus. The video is 1 minute and 44 seconds in length.

b. File name: IMG_1499.MOV
Description: This video depicts a prepubescent female, who is naked from the waist down and wearing a white shirt with different designs. The child is laying with her back against an adult. The adult is using their fingers to penetrate the girls' exposed anus and vagina area. This video is 32 seconds in length.

18. I determined that Cox Communications, Inc. was the Internet service provider for IP address 68.12.239.130. Pursuant to an administrative subpoena, on September 22, 2022, Cox Communications, Inc. provided the following Internet subscriber information for the IP address 68.12.239.130 on the date and times of the downloads described above:

Name:	Jason Roberts
Address:	8104 W Britton Rd. Apt. 14 Oklahoma City, Oklahoma 73132
Phone:	(405) 584-8154
Activation Date:	06/11/2022
Account Status:	Active

19. On July 13, 2022, law enforcement conducted another online undercover investigation on a computer using the IP address 68.12.239.130 because it was associated with a torrent file which referenced 1,601 files, at least one of which had been identified as a file of interest in child pornography investigations.

20. On July 13, 2022, between 20:02 and July 14, 2022, at 02:51 hours, Central Daylight Savings Time, law enforcement completed single-source downloads of approximately 64 files that the device using IP address 68.12.239.130 was making available for others to download on the BitTorrent network. Each of the files was downloaded directly from the device using IP address 68.12.239.130. Based upon my training and experience, I determined that several of these files depict children under the age of eighteen years engaged in sexually explicit conduct that constitutes child pornography as defined by Title 18, U.S.C. § 2256. Two of these files are described below:

a. Filename: (Toddler).Cbaby.4Yo.(Pthc).(Hussyfan).(Raygold).(Abused).Abuse.Chiddy.avi
Description: This video depicts a prepubescent female forced to swallow semen from an adult male ejaculating in her mouth. The video is 34 seconds in length.

b. Filename: Tara Video 4(private7yo).avi
Description: This video depicts a prepubescent female wearing a pink sports bra and pink bottoms. The girl begins to use her fingers to penetrate her exposed vagina. There is a male voice, speaking in English, in the background of the video. The video is 1 minute and 16 seconds in length.

21. On November 15, 2022, law enforcement executed a federal search warrant at the SUBJECT PREMISES. Prior to the execution of the search warrant, law enforcement observed Jason Roberts exit the SUBJECT PREMISES and walk towards his vehicle. At that time, law enforcement detained Jason Roberts and seized his cell phone which was located on his person. During the search at the SUBJECT PREMISES, law enforcement previewed an external hard drive

which was located in Jason Roberts's bedroom, in his nightstand. During the preview, law enforcement identified numerous videos of child pornography and over 100 video titles containing the phrase, "pthc", which stands for pre-teen hard core. Based on the child pornography videos found in Jason Roberts's bedroom, the fact that digital files can be transferred back and forth between digital file storage devices (such as cell phones and traditional computers), and my training and experience that individuals who collect child pornography store them on their digital devices, I believe the cell phone on Jason Roberts person, the SUBJECT DEVICE, will also contain evidence of child pornography. For this reason, I am seeking authorization to search the SUBJECT DEVICE.

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

22. Based on my knowledge, training, and experience in child investigations, and the experience and training of other law enforcement officers with whom I have had discussions, computers, computer technology, and the Internet have revolutionized the manner in which child pornography is produced and distributed.

23. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

24. Child pornographers can transpose photographic images from a camera into a computer-readable format with a scanner. With digital cameras, the images can be transferred directly onto a computer. A modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Through the Internet, electronic contact can be made to millions of computers around the world.

25. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution.

26. The Internet affords collectors of child pornography several different venues for obtaining, viewing and trading child pornography in a secure and anonymous fashion.

27. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail. These online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in a variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer in most cases.

28. As with most digital technology, communications made from a computer are often saved or stored on that computer. Storing this information can be intentional, for example, by saving an e-mail as a file on the computer or saving the location of one's favorite websites in "bookmarked" files. Digital information can also be retained unintentionally. Traces of the path of an electronic communication may be automatically stored in many places. In addition to electronic communications, a computer user's Internet activities generally leave traces in a computer's web cache and Internet history files. A forensic examiner often can recover evidence that shows whether a computer contains peer-to-peer software, when the computer was sharing

files, and some of the files that were uploaded or downloaded. Such information is often maintained indefinitely until overwritten by other data. Likewise, devices such as cellular telephones, tablets, and e-readers are also capable of electronic storage as computers. I know that digital files can be easily moved back and forth between digital file storage devices or stored simultaneously on multiple digital file storage devices. Here, Roberts could have easily transferred files from, for example, a hard drive, to the SUBJECT DEVICE—and vice-versa.

CHILD PORNOGRAPHY COLLECTOR CHARACTERISTICS

29. The following indicates characteristics of child pornography collectors that I have learned through training, working multiple investigations involving child pornography, and from other law enforcement officers:

a. The majority of individuals who collect child pornography are persons who have a sexual attraction to children. They receive sexual gratification and satisfaction from sexual fantasies fueled by depictions of children that are sexual in nature.

b. The majority of individuals who collect child pornography collect sexually explicit materials, which may consist of photographs, magazines, motion pictures, video tapes, books, slides, computer graphics or digital or other images for their own sexual gratification. The majority of these individuals also collect child erotica, which may consist of images or text that do not rise to the level of child pornography but which nonetheless fuel their deviant sexual fantasies involving children.

c. The majority of individuals who collect child pornography often seek out like-minded individuals, either in person or on the Internet, to share information and trade depictions

of child pornography and child erotica as a means of gaining status, trust, acceptance and support. The different Internet-based vehicles used by such individuals to communicate with each other include, but are not limited to, P2P, e-mail, e-mail groups, bulletin boards, IRC, newsgroups, instant messaging, and other similar vehicles.

d. The majority of individuals who collect child pornography maintain books, magazines, newspapers and other writings on the subject of sexual activities with children as a way of understanding their own feelings toward children, justifying those feelings, and finding comfort for their illicit behavior and desires. Such individuals rarely destroy these materials because of the psychological support they provide.

e. The majority of individuals who collect child pornography often collect, read, copy or maintain names, addresses (including e-mail addresses), phone numbers, or lists of persons who have advertised or otherwise made known in publications and on the Internet that they have similar sexual interests. These contacts are maintained as a means of personal referral, exchange or commercial profit. These names may be maintained in the original medium from which they were derived, in telephone books or notebooks, on computer storage devices, or merely on scraps of paper.

f. The majority of individuals who collect child pornography rarely, if ever, dispose of their sexually explicit materials and may go to great lengths to conceal and protect from discovery, theft, and damage their collections. They almost always maintain their collections in the privacy and security of their homes or other secure location.

h. The very nature of this specialized P2P software program is to share files in an attempt to increase a user's collection of files. The software is only successful if the users are sharing their collections so that each user can obtain copies of images and make available their images, and so that all users benefit and increase their collection of images.

CONCLUSION

30. Based on the above information, there is probable cause to believe that the foregoing laws have been violated, and that the property, evidence, fruits, and instrumentalities of these offenses are located on the SUBJECT DEVICE.

31. Based upon the foregoing, I respectfully request that this Court issue a search warrant for the SUBJECT DEVICE, described in Attachment A, authorizing the seizure of the items described in Attachment B to this affidavit.

Marisol Flores
Special Agent
Federal Bureau of Investigation

SUBSCRIBED AND SWORN to before me this 17th day of November, 2022.

Amanda Maxfield-Green
United States Magistrate Judge

ATTACHMENT A

DESCRIPTION OF CELL PHONE

- **Black Samsung Cell Phone with IMEI: 353967950684376**

ATTACHMENT B

LIST OF ITEMS TO BE SEIZED

1. Any and all notes, documents, records, or correspondence, in any format and medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes) pertaining to the possession, receipt, or distribution of child pornography as defined in 18 U.S.C. § 2256(8) or to the possession, receipt, or distribution of visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2).

2. In any format and medium, all originals, computer files, copies, and negatives of child pornography as defined in 18 U.S.C. § 2256(8), visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2), or child erotica.

3. Any and all diaries, address books, names, and lists of names and addresses of individuals who may have been contacted by the operator of the SUBJECT DEVICES or by other means for the purpose of distributing or receiving child pornography as defined in 18 U.S.C. § 2256(8) or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2).

4. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes), identifying persons transmitting, through interstate or foreign commerce by any means, including, but not limited to, by the United States Mail or by computer, any child pornography as defined in 18 U.S.C. § 2256(8) or any visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

5. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, other digital data files and web cache information) concerning the receipt, transmission, or possession of child pornography as defined in 18 U.S.C. § 2256(8) or visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

6. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) concerning communications between individuals about child pornography or the existence of sites on the Internet that contain child pornography or that cater to whose with an interest in child pornography.

7. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) concerning membership in online groups, clubs, or services that provide or make accessible child pornography to members.

8. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern any accounts with an Internet Service Provider.

9. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote

computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage.

10. Any and all address books, mailing lists, supplier lists, mailing address labels, and any and all documents and records, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files), pertaining to the preparation, purchase, and acquisition of names or lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate or foreign commerce by any means, including by the United States Mail or by computer, any child pornography as defined in 18 U.S.C. § 2256(8) or any visual depiction of minors engaged in

11. Any and all diaries, notebooks, notes, and any other records reflecting personal contact and any other activities with minors visually depicted while engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).